



**MPT**  
Technology platform

## **MPT UTM**

Full feature overview including high-end features such as high availability, traffic shaping, intrusion detection and easy VPN client setup. Installation, Design, Configuration and Support is proudly delivered by MPT Saudi Arabia.

**MPT has an innovative NGFW built using various technologies, this is a user-friendly firewall, with many modern features and routing platform that combines the extensive features of commercial products, ranging from a stateful firewall to web application control and integrated inline intrusion detection and prevention. Based on High End BSD for long-term support, our focus on security brings unique features such as an easy to use one time password authentication for various components. Through its modular design and With MVC Model View Controller framework the product is extendible, and API functionality is readily available.**

**The robust and reliable update mechanism gives NGFW the ability to provide important security updates in a timely fashion.**

## **Table of contents**

<b>1. Firewall and Security</b>	<b>3</b>
<b>2. VPN and Remote Access</b>	<b>4</b>
<b>3. Web and Email Security</b>	<b>4</b>
<b>4. Management and Reporting</b>	<b>5</b>
<b>5. High Availability and Clustering</b>	<b>5</b>
<b>6. Cloud and Virtualization</b>	<b>6</b>
<b>7. Authentication and Access Control</b>	<b>6</b>
<b>8. Network Services</b>	<b>6</b>
<b>9. Central Management &amp; Automation</b>	<b>7</b>
<b>10. Diagnostics &amp; Troubleshooting</b>	<b>7</b>
<b>11. Documentation &amp; Support</b>	<b>10</b>
<b>12. Compliance</b>	<b>10</b>

# Categorized List of NGFW Features

## 1. Firewall and Security

Feature	Description	Remark
<b>Stateful Firewall</b>	Supports stateful packet inspection for filtering traffic based on rules and policies.	
<b>Firewall Aliases</b>	Simplifies management of firewall rules using aliases for IP addresses, networks, ports, MACs, GeoIP and BGP ASN, etc.	
<b>Time-based Firewall Rules</b>	Allows firewall rules to be active only during specified times or schedules.	
<b>Port Forwarding and NAT</b>	Configures Network Address Translation for inbound and outbound traffic.	
<b>Traffic Shaping</b>	Manages bandwidth and prioritizes traffic using queues and schedules.	
<b>Policy-Based Routing</b>	Routes traffic based on defined policies and criteria (Source Routing).	
<b>Static Routing</b>	Configure static routes and manually control the path that traffic takes through the network.	
<b>Bridging</b>	Create a layer-2 bridge. Can be configured with (Rapid) Spanning Tree Protocol (RSTP/RTP).	
<b>Anti DDOS</b>	DDoS protection using SYN cookies.	
<b>Static ARP &amp; NDP</b>	Statically configure Address Resolution Protocol (ARP) and Neighbor Discovery Protocol (NDP) and control to which (physical) machine an IP address is connected.	
<b>GeoIP Blocking</b>	Blocks or allows traffic based on geographical location using MaxMind GeoLite2 databases.	Enterprise Edition (or plugin for CE)
<b>Bogon Network Blocking</b>	Blocks traffic from bogon (unallocated or private) IP address spaces.	
<b>Intrusion Detection and Prevention</b>	Network-based intrusion detection and prevention using Suricata.	
<b>Packet Capture and Analysis</b>	Captures and analyzes network traffic at the packet level for troubleshooting and security analysis.	
<b>Traffic Normalization</b>	Protects internal machines against inconsistencies in Internet protocols and implementations.	
<b>Granular State Table Control</b>	Granular control over state table size, rule bases limitations (connections, connection per second, timeout, state type) and optimization options (Normal, High latency, etc.)	
<b>802.1Q VLAN</b>	Support upto 4096 vlans per interface and additionally QinQ 802.1ad is supported by stacking a vlan on top of a vlan.	
<b>VXLAN</b>	Support for Virtual eXtensible Local Area Networks (VXLANs)	
<b>GIF/GRE</b>	Both Generic Routing Encapsulation as well as Generic Tunnel Interfaces are supported.	
<b>Loopback</b>	Logical virtual interfaces which emulate real interfaces and can be used for different setup scenario's, which require always-on interfaces	
<b>Virtual IP configuration</b>	Add extra addresses to already defined interfaces using virtual IPs.	
<b>Advanced Routing</b>	Supports dynamic routing protocols like BGP, IS-IS, LDP, OSPF, PIM and RIP via the FRR plugin.	Plugin
<b>Policy Organization</b>	Support Interface Groups and Rule Categorization	

## 2. VPN and Remote Access

Feature	Description	Remark
<b>OpenVPN Support</b>	Provides site-to-site and remote access VPN using OpenVPN protocol with SSL/TLS encryption. Includes easy to use client export.	
<b>IPsec VPN</b>	Supports IPsec VPN for secure site-to-site and remote access connections.	
<b>WireGuard VPN</b>	Lightweight and high-performance VPN protocol support. Includes an easy to use QR code generator for client configuration.	
<b>Other VPN options</b>	Openconnect, Stunnel, Tinc, ZeroTier (SDWAN/commercial)	Plugin
<b>Dynamic DNS Integration</b>	Keeps VPN endpoints reachable with dynamic IP addresses by updating DNS records automatically. FULLY customised by us.	
<b>Multi-Factor Authentication</b>	Enhances VPN security with additional authentication methods like TOTP (Time-based OTP).	
<b>VPN Road Warrior Setup</b>	Allows mobile clients to connect securely from remote locations.	

## 3. Web and Email Security

Feature	Description	Remark
<b>Web Application Firewall</b>	Easily protect webservices against all sort of injection attacks and provides encryption for traffic to and from the outside world.	Enterprise Edition
<b>Web Proxy (Squid)</b>	Caches web content and enforces access control policies for HTTP/HTTPS traffic.	Plugin
<b>URL Filtering</b>	Controls access to websites based on URLs, domains, and categories using blacklists.	Plugin
<b>Transparent Proxy Mode</b>	Redirects traffic without configuring client browsers.	Plugin
<b>ICAP Support</b>	Integrates with external content adaptation services for advanced filtering.	Plugin
<b>DNS Filtering and Security</b>	Protects against DNS-based threats using DNS over TLS and blocking malicious domains.	
<b>Fine grained DNS filtering</b>	Configure DNS blocking policies in a more fine-grained manner by specifying networks on which the blocklists should apply.	Enterprise Edition
<b>Web Filtering and Control</b>	Filters web content using Squid proxy and URL filtering with blacklists and whitelists.	Plugin
<b>Antivirus Integration</b>	Provides antivirus scanning for web traffic passing through the proxy (ClamAV).	Plugin
<b>SSL Inspection</b>	Decrypts and inspects SSL/TLS traffic using Squid proxy with SSL bumping capabilities.	Plugin
<b>SMTP Proxy</b>	Filters and routes email traffic to protect against spam and malware.	Plugin
<b>Email Antivirus and Antispam</b>	Scans email for viruses and spam using integrated tools like ClamAV and SpamAssassin.	Plugin
<b>Let's Encrypt Integration</b>	Automates SSL/TLS certificate issuance and renewal for secure web access.	Plugin & Enterprise Edition

## 4. Management and Reporting

Feature	Description	Remark
Console administration	Console access is available via serial & SSH. Several features can be controlled from a text based menu including basic setup and firmware upgrade.	
User Identity and Group Management	Manages users and groups locally or integrates with LDAP/RADIUS for authentication and policy enforcement.	Plugin
Role-Based Administration	Defines administrative roles with specific permissions for multi-user management.	
Two-Factor Authentication	Enhances login security using methods like TOTP or hardware tokens.	
Firmware Management	Automatic updates and easy firmware management via web interface or console.	
Configuration Backup and Restore	Allows backing up and restoring configurations locally or to cloud services like Google Drive, Git & NextCloud	Local: Integrated / External: Plugin
Snapshots	Space-efficient and easy to manage full system snapshot.	
Dashboard and Reporting	Web-based dashboard with customizable widgets and detailed reporting tools.	
Netflow Reporting (Insight)	Flexible and fast Netflow Analyzer with drill down and export functionality.	
NetFlow Exporter	Exports network flow data for traffic analysis using external collectors.	
Live Traffic Monitoring	Streaming live traffic graph with both egress and ingress traffic. Selectable interfaces, update timing. Shows both total bandwidth per interfaces as well as per host. Also includes a Top Talkers overview in a tabular form.	
System Health	Monitors system performance and generates graphical statistics over time.	
Logging and Diagnostics	Comprehensive logging facilities with search and filtering capabilities.	
Remote Logging	Comprehensive remote logging with application and level selection. Supports UDP & TCP & Encrypted TLS via IPv4 and IPv6.	
Monitor Service Monitoring	Monitors services and system resources, and sends alerts based on defined conditions.	
APIs and Automation	Provides REST API for automating configuration and management tasks.	

## 5. High Availability and Clustering

Feature	Description	Remark
CARP Failover	Provides failover and redundancy using Common Address Redundancy Protocol (CARP).	
pfsync State Synchronization	Synchronizes firewall states between clustered firewalls for seamless failover.	
High Availability Sync	Synchronizes configuration between primary and secondary firewalls in a high availability setup.	
Load Balancing	Distributes incoming network traffic across multiple servers. Several options are available including relayd and Web Application Firewall (Business Edition)	Plugin
Multi-WAN Load Balancing	Balances outbound traffic across multiple WAN connections for redundancy and bandwidth.	
Gateway Quality Monitoring	Gateway monitoring includes RTT(d) and Loss.	
Link Aggregation (LAGG)	Combines multiple network interfaces for increased bandwidth and redundancy.	

## 6. Cloud and Virtualization

Feature	Description	Remark
<b>Virtualization Support</b>	Runs on various hypervisors like VMware, Hyper-V, Proxmox, and VirtualBox.	
<b>Open Virtual Appliance</b>	Open Virtual Appliance image can be deployed in various virtualization products (e.g. VMware, Virtualbox).	<i>Business Edition</i>
<b>Cloud Deployment</b>	Can be deployed on cloud platforms like AWS and Azure (Marketplace)	
<b>VMware &amp; Xen Integration</b>	Supports open-vm-tools & xen guest utilities for better integration with VMware and Xen environments.	<i>Plugin</i>

## 7. Authentication and Access Control

Feature	Description	Remark
<b>Local User and Group Management</b>	Manages users and groups locally for authentication and access control.	
<b>LDAP and Active Directory Support</b>	Integrates with external directory services for authentication.	
<b>RADIUS Authentication</b>	Supports RADIUS servers for centralized authentication.	
<b>Captive Portal</b>	Provides a web portal for authenticating users before granting network access.	
<b>Certificate Management</b>	Manages SSL/TLS certificates for authentication and encrypted connection. The trust manager includes Certificate Authority's (CA) and Certificate Revocation Lists (CRL).	
<b>Single Sign-On (SSO)</b>	Limited SSO capabilities through integration with directory services.	
<b>802.1X Authentication</b>	Supports network access control for wired and wireless clients using RADIUS authentication.	<i>Plugin</i>
<b>Authentication Logging</b>	Logs authentication events for auditing and compliance purposes.	

## 8. Network Services

Feature	Description	Remark
<b>DHCP Server and Relay</b>	Provides DHCP services and can relay DHCP requests to external servers.	
<b>DNS Server and Forwarder</b>	Offers DNS resolution services using Unbound or Dnsmasq, supports DNS over TLS.	
<b>Dynamic DNS Client</b>	Updates dynamic DNS services with current IP addresses.	<i>Plugin</i>
<b>NTP Server</b>	Synchronizes time across network devices using Network Time Protocol.	
<b>SNMP</b>	Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment. Support IPv4 and IPv6 / SNMP v1, v2c and v3.	<i>Plugin</i>
<b>IPv6 Support</b>	Full support for IPv6 addressing and routing.	

## 9. Central Management & Automation

Feature	Description	Remark
<b>REST API</b>	REST API with ACL support for many parts of the system.	
<b>Scheduled Job Configuration</b>	Schedule jobs to be executed periodically using a Cron daemon. Jobs are registered in the backend to prevent command injection and privilege escalation.	
<b>Central Management</b>	A flexible and power central management enviroment to manage many firewalls centrally	Enterprise Edition
<b>Multi Tenancy</b>	Create multi tenancy setups using host groups with user access controls.	Enterprise Edition
<b>Central Backups</b>	Centralize automatic configuration backup of all configured hosts.	Enterprise Edition
<b>Provisioning</b>	Provision Users & Groups, Aliases, Firewall rules & categories and NAT	Enterprise Edition
<b>Firmware status &amp; control</b>	Report local firmware version and remotely upgrade.	Enterprise Edition
<b>Remote control services</b>	Monitor local services and conrol them (start/stop)	Enterprise Edition
<b>Monitoring</b>	Central monitoring of resource usage, such as CPU, Memory, state table, aliases as wel as bandwidth.	Enterprise Edition
<b>Automatic Login</b>	Use the configured trust to login on the remote hosts WebGUI with a single click.	Enterprise Edition

## 10. Diagnostics & Troubleshooting

Feature	Description	Remark
<b>System Health</b>	Provides detailed graphs and statistics on system performance metrics like CPU usage, memory, disk I/O, and network throughput over time.	
<b>Logging</b>	Comprehensive logging for system events, firewall actions, VPN connections, and services, accessible via the web interface.	
<b>System Logs (Settings)</b>	Configures log settings, such as log retention times and remote syslog servers, for better log management and analysis.	
<b>Logs (General)</b>	Accesses logs for various services like DHCP, VPN, IPSec, PPPoE, and more, facilitating troubleshooting of specific services.	
<b>PPP Log</b>	Shows logs specific to Point-to-Point Protocol connections, useful for troubleshooting WAN links like PPPoE or L2TP.	
<b>Firmware Update Logs</b>	Provides logs related to firmware updates, useful for diagnosing issues during updates.	
<b>Unbound DNS Logs</b>	Shows logs for the Unbound DNS resolver service, helping troubleshoot DNS resolution problems.	
<b>VPN Status and Logs</b>	Provides status and logs for VPN connections (OpenVPN, IPsec, WireGuard), aiding in troubleshooting connectivity issues.	
<b>Cron Logs</b>	Shows logs related to scheduled tasks configured in the Cron daemon, aiding in troubleshooting automation scripts.	
<b>Monit Service Monitoring Logs</b>	Provides logs from Monit, which monitors services and system resources, helping diagnose service failures or resource issues.	
<b>Dynamic DNS Logs</b>	Shows logs related to Dynamic DNS updates, helping diagnose issues with hostname updates.	Plugin
<b>Proxy Server Logs</b>	Displays access and error logs for the proxy server (Squid), useful for diagnosing web access issues.	Plugin

Feature (Continued)	Description	Remark
<b>Intrusion Detection Alerts</b>	Displays alerts generated by the IDS/IPS system (Suricata), including details about detected threats and actions taken.	
<b>High Availability Sync Logs</b>	Displays logs related to configuration synchronization between primary and secondary nodes in high-availability setups.	
<b>ACME Client Logs</b>	Shows logs from the ACME client used for obtaining SSL/TLS certificates from Let's Encrypt, helping diagnose certificate issuance issues.	Plugin
<b>DNSCrypt-Proxy Logs</b>	If using DNSCrypt, displays logs related to encrypted DNS queries and responses, aiding in DNS troubleshooting.	Plugin
<b>Firewall Log View</b>	Displays real-time and historical firewall logs, allowing you to filter and search for specific entries based on criteria like interface, source, destination, and port.	
<b>Firewall Live View</b>	Offers a live view of firewall logs with auto-refresh and color-coded entries for easier analysis of ongoing network activity.	
<b>Packet Capture</b>	Allows capturing network packets on selected interfaces with options to filter by protocol, host, or port; captures can be downloaded for analysis in tools like Wireshark.	
<b>Traffic Graphs</b>	Visualizes real-time network traffic on interfaces, showing bandwidth usage and packet rates.	
<b>Interfaces Statistics</b>	Provides detailed statistics for each network interface, including errors, collisions, and packet counts.	
<b>Ping Utility</b>	Enables you to send ICMP echo requests to test connectivity to a host; supports IPv4 and IPv6.	
<b>Traceroute Utility</b>	Traces the route packets take to reach a destination host, helping identify network path issues; supports IPv4 and IPv6.	
<b>DNS Lookup</b>	Resolves domain names to IP addresses and vice versa, useful for testing DNS functionality.	
<b>NDP Table</b>	Displays the IPv6 Neighbor Discovery Protocol table, showing IPv6 addresses and their corresponding MAC addresses.	
<b>ARP Table</b>	Shows the Address Resolution Protocol table, mapping IP addresses to MAC addresses for IPv4.	
<b>State Table</b>	Lists all active connection states maintained by the firewall, including source, destination, protocol, and interface.	
<b>States Summary</b>	Provides a summarized view of the state table, showing counts of states per protocol, source, and destination.	
<b>Test Port Utility</b>	Checks the connectivity to a specified port on a remote host, useful for testing whether services are reachable.	
<b>Routing Table</b>	Displays the current routing table, showing destination networks, gateways, and interface associations.	
<b>System Activity (Top)</b>	Shows real-time system processes and their CPU and memory usage, similar to the Unix top command.	
<b>NetFlow Exporter</b>	Exports NetFlow data for detailed traffic analysis; can be used with external collectors for in-depth traffic monitoring.	
<b>Firmware Audit</b>	Checks the integrity and versions of installed packages and plugins, ensuring system components are up-to-date and not corrupted.	
<b>Backup &amp; Restore</b>	Allows you to backup the current configuration and restore previous configurations, useful for recovering from misconfigurations.	
<b>Configuration History</b>	Tracks changes made to the system configuration, allowing you to view and revert to previous configurations.	



Feature (Continued)	Description	Remark
<b>DHCP Leases</b>	Displays current DHCP leases, both active and expired, showing IP addresses, MAC addresses, and lease times.	
<b>Sessions (Diagnostics)</b>	Shows currently logged-in users and their session details, including login time and IP address.	
<b>CARP (Status)</b>	Displays Common Address Redundancy Protocol status, useful in high-availability setups to monitor master and backup states.	
<b>Gateway Status</b>	Monitors the status of network gateways, showing latency and packet loss statistics; useful for identifying WAN issues.	
<b>NTP Status</b>	Displays Network Time Protocol synchronization status, including peers and offsets, crucial for time-sensitive operations.	
<b>Services Status</b>	Lists the status of all services running on the firewall, allowing you to start, stop, or restart services as needed.	
<b>Aliases (Diagnostics)</b>	<b>Resolves and lists the current content of aliases, which can be hostnames, networks, or ports used in firewall rules.</b>	
<b>Traffic Shaper Status</b>	Shows the status of traffic shaping queues and their usage, helpful for diagnosing traffic prioritization problems.	
<b>IPsec SAD and SPD</b>	Displays Security Association Database (SAD) and Security Policy Database (SPD) for IPsec VPN connections, essential for VPN troubleshooting.	
<b>Captive Portal Sessions</b>	Displays active captive portal sessions, including user information and session duration.	
<b>User Authentication Tester</b>	Allows testing of user authentication against configured authentication servers like LDAP, RADIUS, or local database.	
<b>Mail Queue Viewer</b>	Displays the status of the mail queue if the firewall is configured to send emails, aiding in troubleshooting email notifications.	<i>Plugin</i>
<b>DHCPv6 Leases</b>	Lists current DHCPv6 leases, similar to DHCP leases but for IPv6 addresses.	
<b>Route Lookup Tool</b>	Determines which gateway or interface traffic to a specific IP address will use, aiding in routing troubleshooting.	
<b>CARP Diagnostics</b>	Provides tools and logs specific to CARP, including pfsync and synchronization status in high-availability setups.	
<b>Wireless Survey</b>	Scans for available wireless networks and displays signal strength and channel usage, useful for wireless network planning and troubleshooting.	
<b>Disks Health and Usage</b>	Monitors disk space usage and health, alerting when thresholds are exceeded to prevent system issues due to disk space exhaustion.	<i>Plugin</i>
<b>Syslog Export</b>	Configures and monitors the export of syslog data to external servers for centralized logging and analysis.	
<b>System Patches</b>	Allows for applying and managing system patches, which can be necessary for fixing specific issues or applying custom changes.	<i>CLI / Console base tools</i>

## 11. Documentation & Support

Feature	Description	Remark
<b>E-Book (English &amp; German)</b>	The complete Practical Firewall	<i>Enterprise Edition</i>
<b>E-learning</b>	Hands-On Labs for Beginners	<i>Enterprise Edition</i>
<b>Online Documentation</b>	Fully searchable online documentation with example setups.	
<b>Online Forum</b>	Online User Forum	
<b>Commercial Support</b>	Commercial support for configuration and trouble shooting.	<i>Enterprise Edition (preferred)</i>

## 12. Compliance

Feature	Description	Remark
<b>LINCE compliance testing</b>	External / 3rd party LINCE compliance testing (jtsec)	<i>Enterprise Edition</i>